



POST-QUANTUM CRYPTOGRAPHY FREQUENTLY ASKED QUESTIONS



1

What is the threat quantum computing poses to current cryptography?

Some of the current cryptographic algorithms currently in use to conduct business online, communicate securely, and digitally sign transactions will be vulnerable if and when a strong enough quantum computer is created. A quantum machine's ability to find the cryptographic key used in these crypto operations could be used by an adversary to then decrypt and read or falsify a document.

2

Why is post-quantum cryptography important for my organization now? Why do we need to begin planning right now?

As we have learned from previous transitions, large transitions of cryptographic technologies take time and are complex. Planning now for this change in foundational security capabilities will ensure your organization is secure when a cryptographically relevant machine is created. Working with the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) to understand, plan, and prioritize is the key first step. ¹

3

What cryptography protocols are vulnerable to a quantum computer? Is all cryptography vulnerable to quantum computing-based attacks?

No, not all encryption is vulnerable and much of the current encryption we use will still be effective. Specifically, our current public key cryptographic systems that use digital signatures (FIPS 186) and public key-based key establishment mechanisms (NIST SP 800-56A/B/C), as well as related protocols, will be vulnerable. Symmetric key based crypto systems are not vulnerable. The security strength can be reduced by quantum attacks using Grover's Algorithm; however, this can be addressed by increasing the key sizes, which is the focus of NIST's current efforts to identify quantum-resistant algorithms. These include Advanced Encryption Standard, Secure Hash Algorithm, High-Based Message Authentication Code, and other cryptographic key management techniques.

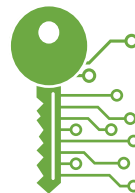
4

A quantum computer will need how many stable qubits to be cryptographically relevant?

For a quantum computer to run Shor's Algorithm and break a public key it will need an estimated 6,000 stable qubits. Qubits are extremely fragile and can interact with the external environment introducing errors or noise. The point at which a given quantum computer is built with sufficient qubit capacity to break public key cryptography sometimes called "cryptographically relevant", when a quantum machine now can break our current cryptographic algorithms. This is still significantly larger in size and power than a quantum machine that achieves "quantum supremacy." ²

¹ <https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography>

² Fortune Magazine defined Quantum supremacy in 2019 as researchers have been able to use a quantum computer to perform a single calculation that no conventional computer, even the biggest supercomputer, can perform in a reasonable amount of time.





5

When will a cryptographically relevant quantum computer be available?

This is currently unknown, but continued progress in quantum engineering is occurring. Google has publicly set a goal of building a 1,000 stable qubit machine by the end of the 2020 decade.³

6

Should I procure commercial post-quantum cryptography solutions now?

No. Organizations should wait until strong, standardized commercial solutions are available that implement the upcoming NIST recommendations to ensure interoperability as well as solutions that are strongly vetted and globally acceptable.

7

When will an approved post-quantum cryptography standard be released publicly?

NIST plans to publish standards for post-quantum cryptography in 2024 and at that point, commercial products will be available using those standards.

8

What are we doing today to protect our information against future exploitation by quantum computers?

First, plan for your transition. NIST and DHS will be working on several projects to assist organizations in that planning. A key part of this planning is to understand the needs for future-proofing the confidentiality of encrypted information that is sent over unsecure networks and ensuring you prioritize your post-quantum transition properly. Some standards are available for very specific needs and use cases. NIST has recommended the IETF standards for hash-based signatures as an example (see NIST SP 800-208). Organizations should plan for “cryptographic agility” in any new product they procure. This is ensuring that the encryption is easily upgraded or replaced and not hard coded in products.

9

What is DHS’s Role in Post Quantum Cryptography Transition?

In partnership with NIST, DHS is focusing on three main workstreams. First, DHS is taking action to prepare internally for the transition to post-quantum cryptography. Second, DHS is working closely with NIST to develop specific guidance for individual organizations to prepare for the transition. Third, DHS, through the Cybersecurity and Infrastructure Security Agency (CISA), is conducting a macro-level analysis of National Critical Functions to identify which sectors and organizations should prioritize preparing for this transition and which entities may need support from the government to ensure a smooth and equitable transition.

10

What is involved in replacing quantum-vulnerable cryptography?

This will require an update to cryptographic infrastructures, coordinated with industry and other agencies. It will require allocation of resources, careful planning, and a time where organizations will operate in a dual mode while partners and collaborators make their needed upgrades as well. This will be a multi-year process that will require continuous engagement, communicate and assist everyone with making this a successful transition.

³ <https://blog.google/technology/ai/unveiling-our-new-quantum-ai-campus/>

